arXiv:1112.1137v2 [quant-ph] 19 Sep 2012

Structural Characterization And Condition For Measurement Statistics Preservation Of A Unital Quantum Operation

Kai-Yan Lee,* Chi-Hang Fred Fung,† and H. F. Chau‡

Department of Physics and Center of Computational and Theoretical Physics
University of Hong Kong, Pokfulam Road, Hong Kong

(Dated: September 20, 2012)

We investigate the necessary and sufficient condition for a convex cone of positive semidefinite operators to be fixed by a unital quantum operation ϕ acting on finite-dimensional quantum states. By reducing this problem to the problem of simultaneous diagonalization of the Kraus operators associated with ϕ, we can completely characterize the kind of quantum states that are fixed by ϕ. Our work has several applications. It gives a simple proof of the structural characterization of a unital quantum operation that acts on finite-dimensional quantum states — a result not explicitly mentioned in earlier studies. It also provides a necessary and sufficient condition for what kind of measurement statistics is preserved by a unital quantum operation. Finally, our result clarifies and extends the work of Størmer by giving a proof of a reduction theorem on the unassisted and entanglement-assisted classical capacities, coherent information, and minimal output Renyi entropy of a unital channel acting on finite-dimensional quantum state.

PACS numbers: 03.67.Hk, 02.10.Yn, 03.65.Aa

I. INTRODUCTION

A quantum channel can be modeled by a quantum operation ϕ on a separable Hilbert space $\mathcal{H}$. Mathematically, $\phi\colon \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ is a trace-preserving completely positive map on the set of all bounded operators of $\mathcal{H}$. Characterizing quantum operations and studying their properties are two important areas of research in quantum information science. Nevertheless, many apparently simple and basic questions regarding a quantum operation are difficult to answer. One example is to find all quantum states ρ (in other words, trace one positive self-adjoint operators) that are fixed points of a given quantum operation in the sense that $\phi(\rho) = \rho$. This question is still open. Recently, some progress has been made on attacking this question. Kribs [1], who used simple functional analysis argument, and Arias *et al.* [2], who applied the generalized Lüders theorem, independently discovered a useful necessary and sufficient condition for a class of quantum channels known as unital quantum operations to fix a quantum state provided that the dimension of the Hilbert space $\mathcal{H}$ is finite. Studies on the generalization and limitations of Arias *et al.*'s result along the line of generalized Lüders theorem have also been reported. [3–10]

Restricting the study to unital rather than general quantum channels is a sensible tactic to make progress. This is because many physical processes in actual experiments such as depolarization and dephasing can be modeled by unital channels so that it is worthwhile to study these channels. Besides, the mathematical tools and results to deal with unital quantum operations are reasonably well-developed. Therefore, it is not surprising that several quantum information science problems involving unital quantum operations have been solved. For example, by means of finite-dimensional C^*-algebra, Størmer found that the evaluation of the (unassisted) classical capacity $C_{1,\infty}$ of a unital quantum channel acting on finite-dimensional quantum states can be reduced to calculating the same channel capacity for the case in which the image of a non-scalar projection is never a projection. [11] In another study, Blume-Kohout *et al.* used unital quantum channel as an auxiliary tool and results from matrix algebra to characterize the geometric structure of noiseless subsystems, decoherence-free subspaces, pointer bases and quantum error-correcting codes acting on finite-dimensional quantum states. The geometric structure they have identified is an isometry to fixed points of certain unital quantum operations. [12, 13] They also extended their results by showing several interesting properties of the set of fixed points of an arbitrary finite-dimensional quantum channel. [13] Using similar techniques, Rosmanis studied the properties of the fixed space of a positive (but not necessarily completely positive) trace-preserving map. [14] Recently, Mendl and Wolf discovered several equivalent definitions for a unital quantum operation and used them to study the relation between unital channels and quantum error corrections. Their results shine new light on the asymptotic Birkhoff conjecture and the separation of the set of mixtures of unitary channels. [15] Lately, Zhang and Wu showed an easily checkable necessary and sufficient condition for a finite-dimensional quantum state whose von Neumann entropy is preserved by a given unital channel. Interestingly, their work is closely related to finding fixed points of the composition of a unital quantum operation ϕ and its adjoint quantum operation. [16]

* Present address: Department of Astronomy and Oskar Klein Centre for Cosmoparticle Physics, Stockholm University, AlbaNova, SE-10691 Stockholm, Sweden; lee.kai_yan@astro.su.se

† chffung@hku.hk

‡ Corresponding author, hfchau@hku.hk

In turns out that the works of Kribs [1], Størmer [11] and Blume-Kohout *et al.* [12, 13] mentioned in the above paragraph are closely related to the following variation of the fixed point problem in which we called the fixed convex cone of positive semidefinite operator problem. Let $\mathcal{B}(\mathcal{H})$ be the set of all bounded operators of a finite-dimensional Hilbert space $\mathcal{H}$. (All Hilbert spaces considered in this paper are of finite dimensions.) And let $\phi\colon \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ be a unital quantum operation. That is to say, $\phi(\rho)$ can always be expressed as a finite sum in the form $\sum_i A_i \rho A_i^\dagger$ known as the operator-sum representation with $\sum_i A_i^\dagger A_i = I_{\mathcal{H}} = \sum_i A_i A_i^\dagger$ so that $\phi(I_{\mathcal{H}}) = I_{\mathcal{H}}$, where $I_{\mathcal{H}}$ denotes the identity operator on $\mathcal{H}$. Surely, A_i's (which are called the Kraus operators associated with ϕ) as well as elements in $\mathcal{B}(\mathcal{H})$ can be regarded as complex-valued matrices of dimension $\dim \mathcal{H} < \infty$ with respect to an orthonormal basis of $\mathcal{H}$. By the fixed convex cone of positive semidefinite operator problem, we refer to the problem of determining if ϕ fixes a convex cone $\mathcal{C}^+$ formed by the set of all positive semidefinite operators in $\mathcal{B}(\mathcal{S})$ for a (proper) Hilbert subspace $\mathcal{S}$ of $\mathcal{H}$ in the sense that $\phi[\mathcal{C}^+] \subset \mathcal{C}^+$. Since ϕ is a trace-preserving completely positive map, our fixed convex cone problem is equivalent to the problem of determining the existence of a subspace $\mathcal{S}$ of $\mathcal{H}$ such that ϕ sends density matrices in $\mathcal{S}$ to density matrices in $\mathcal{S}$ — a problem of quantum information science interest. (Unlike the approaches in Refs. [1, 11–13], we are not interested in the action of ϕ on $\sigma \in \mathcal{B}(\mathcal{H})$ that is not a density matrix because σ does not describe a physical quantum state and hence plays no role in quantum information science.) By abusing language, we call the Hilbert subspace $\mathcal{S}$ an invariant subspace of ϕ; alternatively, we say that ϕ fixes the subspace $\mathcal{S}$. If such a proper subspace $\mathcal{S}$ exists, we would like to explicitly find it out.

Interestingly, we are going to show in Sec. II that if $\mathcal{S}$ is an invariant subspace of a unital quantum operation ϕ, then so is its orthogonal subspace $\mathcal{S}^\perp$. In other words, a unital quantum operation ϕ induces a direct sum decomposition of the finite-dimensional Hilbert space $\mathcal{H}$ into irreducible invariant subspaces (IrIS's) of ϕ. Here an IrIS means that it does not contain any proper invariant subspace. More importantly, we further prove in Sec. II that ϕ fixes the subspace $\mathcal{S}$ (and hence also $\mathcal{S}^\perp$) if and only if $\mathcal{S}$ and $\mathcal{S}^\perp$ are simultaneous invariant subspaces of all Kraus operators A_i's associated with ϕ. That is, $A_i[\mathcal{S}] \subset \mathcal{S}$ and $A_i[\mathcal{S}^\perp] \subset \mathcal{S}^\perp$ for all i. Hence, ϕ has an interesting structure in the sense that it induces a simultaneous block diagonalization for all its Kraus operators A_i's such that each diagonal block acts on a different irreducible invariant subspace of ϕ. In this regard, our notion of convex cone fixation, which concentrates only on the action of ϕ on density matrices, turns out to be strong enough to force $\phi[\mathcal{B}(\mathcal{S})] \subset \mathcal{B}(\mathcal{S})$.

An interesting consequence of this finding is a simple proof of the structural characterization theorem of unital quantum operation acting on finite-dimensional density matrices. As far as we know, we are the first group who explicitly state and prove this theorem although this theorem can be deduced from the works of Kribs [1] and Blume-Kohout *et al.* [13]. Furthermore, both prior works did not investigate the quantum information processing consequences of the structural characterization theorem of finite-dimensional unital quantum operations. In fact, Kribs showed in Lemma 2.2 of Ref. [1] that fixed points for an irreducible unital quantum operation acting on $\mathcal{B}(\mathcal{H})$ with $\dim \mathcal{H} < \infty$ must be scalars. This is a special case of Theorem 2 to be reported in Sec. II. However, Kribs did not mention the decomposition of unital quantum operation into direct sum of irreducible ones and properties of such a decomposition. Whereas in Lemmas 5.4, 5.5 and Theorem 5 of Ref. [13], Blume-Kohout *et al.* used the structure theorem of matrix algebra to prove the existence of a direct sum decomposition structure for a general finite-dimensional quantum operation. They also discussed its implications on the structure of the associated Kraus operators. Our structural characterization theorem can be readily deduced from this work by sharpening their results for the case of a unital operation. Here we use an alternative approach, which uses rather elementary techniques in mathematical analysis and graph theory, to obtain the structural characterization theorem for finite-dimensional unital quantum operations. In this way, we avoid going through the more technical proofs on a more general situation in Refs. [1, 13] and adapting them to our particular case of interest.

The structure theorem reported in Sec. II has a few quantum information science applications. In Sec. III, we first use it to obtain a simple and intuitive proof of a theorem concerning the calculation of classical capacity $C_{1,\infty}$ of a unital channel acting on finite-dimensional quantum states originally obtained by Størmer in Ref. [11]. Our proof can be used to extend Størmer's result to the calculation of the entanglement-assisted classical capacity C_e, the coherent information J, and the minimal output α-Renyi entropy $S_{\min,\alpha}$ of the same channel. More importantly, we completely characterize the kind of quantum states that are fixed by a unital quantum operation in Sec. III. And we provide a necessary and sufficient condition for the measurement statistics of a positive operator-valued measure (POVM) measurement to be preserved when a general finite-dimensional quantum state passes through a unital quantum channel. Finally, we briefly discuss the implications of our results in Sec. IV.

II. STRUCTURAL CHARACTERIZATION OF UNITAL QUANTUM OPERATIONS ACTING ON FINITE-DIMENSIONAL DENSITY MATRICES

We use the following theorem, which was independently proven by Kribs as Theorem 2.1 in Ref. [1] and by Arias *et al.* as Theorem 3.5(a) in Ref. [2], as our starting point to study the existence of invariant subspace of a unital quantum operation. (See also the variation of this

theorem stated as Lemma 5.2 in Ref. [13].)

Theorem 1. *Let $\phi(\cdot) = \sum_i A_i \cdot A_i^\dagger$ be a unital quantum operation on the set of all bounded operators of a finite-dimensional Hilbert space $\mathcal{H}$. Then, ϕ fixes $\sigma \in \mathcal{B}(\mathcal{H})$ (that is, $\phi(\sigma) = \sigma$) if and only if $A_i\sigma = \sigma A_i$ for all i.*

Remark 1. *In particular, Theorem 1 relates fixing a quantum state ρ (a property independent of the choice of the associated Kraus operators A_i's) to the commutativity of ρ with the set of Kraus operators A_i's used any operator-sum representation of the unital quantum operator ϕ. This is possible partly because of a unitary degree of freedom in the operator-sum representation of ϕ. More precisely, $\phi(\cdot) = \sum_i A_i \cdot A_i^\dagger = \sum_i B_i \cdot B_i^\dagger$ if and only if $B_j = \sum_i u_{ij} A_i$ for all j where u_{ij} is the (i,j)-th element of a unitary matrix. [17] Thus, the commutativity of ρ with all A_i's implies the commutativity of ρ with all B_i's.*

A special case of Theorem 1 is that ϕ fixes a (normalized) pure state $|x\rangle$ if and only if $|x\rangle$ is an eigenvector of A_i for all i. (The "if part" can be deduced by the fact that $A_i|x\rangle = \lambda_i|x\rangle$ implies $\phi(|x\rangle\langle x|) = \sum_i |\lambda_i|^2 |x\rangle\langle x| = |x\rangle\langle x|$ for ϕ is trace-preserving. The "only if part" follows from

$$A_i|x\rangle = A_i|x\rangle\langle x|x\rangle = |x\rangle\langle x|A_i|x\rangle = \langle x|A_i|x\rangle\, |x\rangle. \quad (1)$$

Note also that by the same argument in Remark 1, $|x\rangle$ is an eigenvector for any Kraus operators used in the operator-sum representation of ϕ although the corresponding eigenvalues are operator-sum representation dependent.) In other words, ϕ fixes an one-dimensional subspace $\mathcal{S}$ of $\mathcal{H}$ if and only if $\mathcal{S}$ is a simultaneous eigenspace of all its Kraus operators A_i's.

We now apply Theorem 1 to study the necessary and sufficient condition for the existence of invariant subspace of ϕ.

Theorem 2. *Let ϕ be a unital quantum operation on the set of all bounded operators of a finite-dimensional Hilbert space $\mathcal{H}$. Then, ϕ fixes a Hilbert subspace $\mathcal{S}$ of $\mathcal{H}$ if and only if $\phi(P_\mathcal{S}) = P_\mathcal{S}$ where $P_\mathcal{S}$ is the projection operator onto $\mathcal{S}$.*

Proof. ($\Leftarrow$): Assume there exists an Hermitian operator $\sigma_\mathcal{S}$ whose support is in $\mathcal{S}$. Suppose further that $0 \le \sigma_\mathcal{S} \le P_\mathcal{S}$ and $\phi(\sigma_\mathcal{S}) \notin \mathcal{S}$. Then, $\sigma_{\mathcal{S}'} \equiv P_\mathcal{S} - \sigma_\mathcal{S} \ge 0$. More importantly,

$$P_\mathcal{S} = \phi(P_\mathcal{S}) = \phi(\sigma_\mathcal{S}) + \phi(\sigma_{\mathcal{S}'}). \quad (2)$$

Since $\phi(\sigma_\mathcal{S}) \notin \mathcal{S}$, there exists $|x\rangle \in \mathcal{S}^\perp$ such that $\langle x|\phi(\sigma_\mathcal{S})|x\rangle \neq 0$ where $\mathcal{S}^\perp$ denotes the orthogonal complement of $\mathcal{S}$. And by the positivity of $\phi(\sigma_\mathcal{S})$, we have $\langle x|\phi(\sigma_\mathcal{S})|x\rangle > 0$. But then

$$\begin{aligned}\langle x|\phi(\sigma_{\mathcal{S}'})|x\rangle &= \langle x|P_\mathcal{S}|x\rangle - \langle x|\phi(\sigma_\mathcal{S})|x\rangle \\ &= -\langle x|\phi(\sigma_\mathcal{S})|x\rangle < 0. \end{aligned} \quad (3)$$

This is impossible for ϕ is a quantum operation. Therefore, we conclude that $\phi(\sigma_\mathcal{S}) \in \mathcal{S}$ for all non-negative operators on $\mathcal{S}$. In other words, ϕ fixes $\mathcal{S}$.

($\Rightarrow$): ϕ fixes $\mathcal{S}$ implies $\phi(P_\mathcal{S}) \in \mathcal{S}$. Assume the contrary is true so that $\phi(P_\mathcal{S}) \neq P_\mathcal{S}$. Let $P_{\mathcal{S}^\perp} = P_\mathcal{H} - P_\mathcal{S}$ be the projection operator onto the orthogonal complement of $\mathcal{S}$. Then,

$$\phi(P_\mathcal{S}) + \phi(P_{\mathcal{S}^\perp}) = \phi(P_\mathcal{H}) = P_\mathcal{H}. \quad (4)$$

Note that the last equality in the above equation follows from the fact that ϕ is unital. Since $\mathcal{H}$ is finite-dimensional and ϕ fixes $\mathcal{S}$, we can express $\phi(P_\mathcal{S})$ as the finite sum $\sum_{j=1}^{\dim\mathcal{S}} a_j |y_j\rangle\langle y_j|$ with non-negative a_j's, where $\{|y_j\rangle\}$ is an orthonormal basis of $\mathcal{S}$. Since $\phi(P_\mathcal{S}) \neq P_\mathcal{S}$, we cannot have $a_j = 1$ for $j = 1, 2, \ldots, \dim\mathcal{S}$. Nevertheless, since ϕ is trace-preserving, a_j's still have to satisfy the constraint $\sum_{j=1}^{\dim\mathcal{S}} a_j = \dim\mathcal{S}$. Thus, by relabeling the index if necessary, we may assume that $a_1 > 1$ and $a_2 < 1$. So, from Eq. (4),

$$\begin{aligned} 1 &= \langle y_1|\phi(P_\mathcal{S})|y_1\rangle + \langle y_1|\phi(P_{\mathcal{S}^\perp})|y_1\rangle \\ &= a_1 + \langle y_1|\phi(P_{\mathcal{S}^\perp})|y_1\rangle. \end{aligned} \quad (5)$$

That is to say, $\langle y_1|\phi(P_{\mathcal{S}^\perp})|y_1\rangle = 1 - a_1 < 0$, which contradicts the assumption that ϕ is a quantum operation. Therefore, we conclude that $\phi(P_\mathcal{S}) = P_\mathcal{S}$. □

Remark 2. *Note that the unital condition is needed only in the proof of the "only if part" of the Theorem. Note further that Kribs proved the special case of this theorem when ϕ does not fix any proper subspace of $\mathcal{H}$ [1].*

Corollary 1. *ϕ fixes $\mathcal{S}$ if and only if ϕ fixes $\mathcal{S}^\perp$.*

Proof. By Theorem 2 and Eq. (4), ϕ fixes $\mathcal{S}$ if and only if $\phi(P_{\mathcal{S}^\perp}) = P_\mathcal{H} - \phi(P_\mathcal{S}) = P_\mathcal{H} - P_\mathcal{S} = P_{\mathcal{S}^\perp}$, which in turn is true if and only if ϕ fixes $\mathcal{S}^\perp$. □

Corollary 2. *ϕ fixes the subspace $\mathcal{S}$ if and only if*

$$\langle s^\perp|A_i|s\rangle = 0 = \langle s|A_i|s^\perp\rangle \quad (6)$$

for all $|s\rangle \in \mathcal{S}$ and $|s^\perp\rangle \in \mathcal{S}^\perp$ and for all Kraus operators A_i's of ϕ.

Proof. From Theorem 2, ϕ fixes $\mathcal{S}$ implies $\phi(P_\mathcal{S}) = P_\mathcal{S}$. Theorem 1 further implies $A_i P_\mathcal{S} = P_\mathcal{S} A_i$ for all i. Multiplying $\langle s^\perp|$ on the left and $|s\rangle$ on the right gives $\langle s^\perp|A_i|s\rangle = 0$. Similarly, multiplying $\langle s|$ on the left and $|s^\perp\rangle$ on the right gives $\langle s|A_i|s^\perp\rangle = 0$.

To prove the converse, one only needs to observe that Eq. (6) implies $A_i[\mathcal{S}] \subset \mathcal{S}$ for all i. Thus, ϕ fixes $\mathcal{S}$. □

Remark 3. *Surprisingly, the notion of convex cone fixation by a unital quantum operation ϕ is much stronger than what we have originally written down. Recall from Sec. I that ϕ fixes a Hilbert subspace $\mathcal{S}$ simply means $\phi[C_\mathcal{S}^+] \subset C_\mathcal{S}^+$ where $C_\mathcal{S}^+$ denotes the convex cone formed by the set of all positive semidefinite operators in $\mathcal{B}(\mathcal{S})$. Yet, the above two Corollaries say that subspace fixing*

actually demands something more, namely, $\phi[\mathcal{B}(\mathcal{S})] \subset \mathcal{B}(\mathcal{S})$, $\phi[\mathcal{B}(\mathcal{S}^\perp)] \subset \mathcal{B}(\mathcal{S}^\perp)$. *Note further that we cannot directly deduce Corollary 2 from Corollary 1 for the latter says nothing on* $\phi(\sigma)$ *for a general operator* σ *whose support is in* $\mathcal{S}$.

This motivates us to formulate our main theorem.

Theorem 3 (Structural theorem for unital quantum operations on finite-dimensional density matrices).
(a) Every finite-dimensional unital quantum operation $\phi\colon \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ *induces a direct sum decomposition of* $\mathcal{H} = \bigoplus_j \mathcal{S}_j$ *where each* $\mathcal{S}_j$ *is an IrIS of* ϕ. *Furthermore, every Kraus operator* A_i *of* ϕ *can also be decomposed as* $\bigoplus_j A_i^{\mathcal{S}_j}$ *where* $A_i^{\mathcal{S}_j} \in \mathcal{B}(\mathcal{S}_j)$ *for all* i, j. *Hence, the quantum operation* $\phi|_{\mathcal{B}(\mathcal{S})}$ *is also unital whenever* $\mathcal{S}$ *is an invariant subspace of* ϕ. *In other words,* ϕ *can be expressed as a direct sum* $\bigoplus_j \phi|_{\mathcal{B}(\mathcal{S}_j)}$ *of unital quantum operations. In matrix language,* ϕ *has a proper invariant subspace if and only if each of its Kraus operators can be simultaneously block diagonalized by unitary conjugation into at least two diagonal blocks.*
(b) In addition, $\mathcal{S}$ *is an IrIS of* ϕ *if and only if all fixed positive self-adjoint operators of* ϕ *in* $\mathcal{B}(\mathcal{S})$ *are in the form* $aP_{\mathcal{S}}$ *for some* $a \geq 0$, *where* $P_{\mathcal{S}}$ *denotes the projection operator onto* $\mathcal{S}$.

Proof. From Corollaries 1 and 2, every Kraus operator A_i of a unital quantum operator $\phi\colon \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ with $\dim \mathcal{H} < \infty$ admits a direct sum decomposition $A_i^{\mathcal{S}} \oplus A_i^{\mathcal{S}^\perp}$ where $A_i^{\mathcal{S}}$ ($A_i^{\mathcal{S}^\perp}$) is a linear operator in the invariant subspace $\mathcal{S}$ ($\mathcal{S}^\perp$) of ϕ. Since $\sum_i A_i^{\mathcal{S}} A_i^{\mathcal{S}\dagger} = I_{\mathcal{S}}$, the quantum operation $\phi|_{\mathcal{B}(\mathcal{S})}(\cdot) \equiv \sum_i A_i^{\mathcal{S}} \cdot A_i^{\mathcal{S}\dagger}$ is unital. By the same token, $\phi|_{\mathcal{B}(\mathcal{S}^\perp)}(\cdot) \equiv \sum_i A_i^{\mathcal{S}^\perp} \cdot A_i^{\mathcal{S}^\perp\dagger}$ is unital. By recursively applying Corollaries 1 and 2 to the unital quantum operations $\phi|_{\mathcal{B}(\mathcal{S})}(\cdot)$ and $\phi|_{\mathcal{B}(\mathcal{S}^\perp)}$ at most $\dim(\mathcal{H}) - 1$ times, part (a) is proven.

To prove part (b), suppose $0 \leq \sigma \in \mathcal{B}(\mathcal{S})$ is fixed by ϕ and yet $\sigma \neq aP_{\mathcal{S}}$ for all $a \geq 0$. Since $\mathcal{H}$ and hence $\mathcal{S}$ are finite-dimensional, we may write $\sigma = \sum_{j=1}^{\dim \mathcal{S}} b_j |y_j\rangle\langle y_j|$ for some orthonormal basis vectors $|y_j\rangle$'s of $\mathcal{S}$ and all b_j's are non-negative. By relabeling the indices if necessary, may we assume that $b_1 \leq b_j$ for all j; and the requirement that $\sigma \neq aP_{\mathcal{S}}$ implies not all b_j's are equal. Using part (a), $\phi|_{\mathcal{S}}$ is also unital so that ϕ fixes $P_{\mathcal{S}}$ and hence also the operator σ' given by

$$\sigma' = \sigma - b_1 P_{\mathcal{S}} = \sum_{j=2}^{\dim \mathcal{S}} (b_j - b_1)\, |y_j\rangle\langle y_j| > 0. \tag{7}$$

From Theorem 1, $A_i^{\mathcal{S}} \sigma' = \sigma' A_i^{\mathcal{S}}$ for all i. By multiplying $\langle y_1|$ on the left and $|y_j\rangle$ on the right, we get $(b_j - b_1)\langle y_1|A_i^{\mathcal{S}}|y_j\rangle = 0$ for all i, j. Similarly, multiplying $\langle y_j|$ on the left and $|y_1\rangle$ on the right gives $(b_j - b_1)\langle y_j|A_i^{\mathcal{S}}|y_1\rangle = 0$ for all i, j. That is, $\langle y_j|A_i^{\mathcal{S}}|y_1\rangle = \langle y_1|A_i^{\mathcal{S}}|y_j\rangle = 0$ for all i whenever $b_1 < b_j$. Following the same logic, we conclude that

$$\langle y_j|A_i^{\mathcal{S}}|y_k\rangle = \langle y_k|A_i^{\mathcal{S}}|y_j\rangle = 0 \tag{8}$$

for all i whenever $b_1 = b_k < b_j$. Consequently, each of the $A_i^{\mathcal{S}}$'s can be simultaneously block diagonalized by unitary conjugation to at least two diagonal blocks — one block corresponds to those indices k's with $b_k = b_1$ and the other block corresponds to those k's with $b_k > b_1$. From Corollary 2, $\mathcal{S}$ is not an IrIS of $\mathcal{H}$, which is absurd.

Finally, to show the converse of part (b), suppose $\mathcal{S}'$ is a proper subspace of $\mathcal{S}$ that is fixed by ϕ. Then, it is clear from part (a) that ϕ fixes the projection operator $P_{\mathcal{S}'}$. Hence, not all positive self-adjoint operators in $\mathcal{B}(\mathcal{S})$ fixed by ϕ are in the form $aP_{\mathcal{S}}$. This proves the theorem. □

Remark 4. *As we have mentioned in Sec. I, Theorem 3 can also be deduced from the work of Kribs [1] and Blume-Kohout* et al. *[13].*

Remark 5. *The unitary degree of freedom in operator-sum representation mentioned in Remark 1 is the reason why Eq.* (6) *in Corollary 2 as well as the simultaneous block diagonalization of* A_i*'s in part (a) of Theorem 3 hold for any Kraus operators associated with* ϕ.

Remark 6. *Actually, positivity of the self-adjoint operator* σ *is not essential in the proof of part (b) of Theorem 3. In fact, it can be slightly strengthened as* $\mathcal{S}$ *is an IrIS of* ϕ *if and only if all fixed self-adjoint operators of* ϕ *in* $\mathcal{B}(\mathcal{H})$ *are in the form* $aP_{\mathcal{S}}$ *for some* $a \in \mathbb{R}$. *The proof is left to interested readers. We do not state this slightly more general form in the theorem because we are more interested in the action of* ϕ *to a physical quantum state.*

Remark 7. *In general, a matrix can be diagonalized into irreducible blocks in more than one orthonormal basis due to degeneracy of its eigenspace. This is also the reason why the IrIS decomposition of a finite-dimensional unital quantum operation discussed in the above theorem need not be unique.*

The following example illustrates the power of Theorem 3 in determining the structures of some well-known unital quantum channels.

Example 1. *Consider the depolarization qudit channel* ϕ *over a finite-dimensional Hilbert space* $\mathcal{H}$. *That is,* ϕ *sends a density matrix* ρ *to* $(1-p)\rho + pI_{\mathcal{H}}/\dim \mathcal{H}$ *with* $0 < p \leq 1$. *More generally,* $\phi(\sigma) = (1-p)\sigma + pI_{\mathcal{H}} \operatorname{Tr}(\sigma)/\dim \mathcal{H}$ *for all* $\sigma \in \mathcal{B}(\mathcal{H})$. *Let* $P_{\mathcal{S}}$ *be the projector on a Hilbert subspace* $\mathcal{S}$ *of* $\mathcal{H}$. *Then,* ϕ *fixes* $P_{\mathcal{S}}$ *if and only if* $pP_{\mathcal{S}} = pI_{\mathcal{H}} \dim \mathcal{S}/\dim \mathcal{H}$. *As* $p \neq 0$, ϕ *fixes* $P_{\mathcal{S}}$ *if and only if* $\mathcal{S} = \mathcal{H}$. *Since* ϕ *is unital, Theorem 3 implies that* $\mathcal{H}$ *is the only IrIS of* ϕ. *In this regard, all finite-dimensional depolarizing qudit channels cannot be further decomposed as a direct sum of two unital quantum operations.*

Although IrIS decomposition induced by ϕ may not be unique, different IrIS decompositions share the same dimensional structure. This is analogous to the dimensions of IrIS for complex-valued matrices.

Theorem 4. *Suppose* $\mathcal{H} = \bigoplus_{i=1}^m \mathcal{S}_i = \bigoplus_{j=1}^n \mathcal{S}'_j$ *be two different IrIS decompositions induced by* ϕ *reported in part (a) of Theorem 3 indexed in such a way that* $\dim \mathcal{S}_i \geq \dim \mathcal{S}_{i'}$ *whenever* $i > i'$ *and* $\dim \mathcal{S}'_j \geq \dim \mathcal{S}'_{j'}$ *whenever* $j > j'$*. Then* $m = n$ *and* $\dim \mathcal{S}_i = \dim \mathcal{S}'_i$ *for all* i*.*

Proof. Since there are two distinct IrIS decompositions for ϕ, we can always find an IrIS in the first decomposition, say, $\mathcal{S}_1$ that is distinct from all the IrIS's in the second decomposition. As $\mathcal{S}_1 \subset \bigoplus_j \mathcal{S}'_j$, we can find an IrIS in the second decomposition, say $\mathcal{S}'_1$ which is not contained in $\mathcal{S}_1^\perp$ the orthogonal subspace of $\mathcal{S}_1$.

We claim that $\dim \mathcal{S}_1 = \dim \mathcal{S}'_1$. Suppose the contrary, may we assume without lost of generality that $\dim \mathcal{S}_1 > \dim \mathcal{S}'_1$. Let us write $\mathcal{S}_1 = \mathcal{T}_1 \oplus \mathcal{U}_1$ and $\mathcal{S}'_1 = \mathcal{T}'_1 \oplus \mathcal{U}'_1$ where $\mathcal{T}_1 = \mathcal{S}_1 \cap {\mathcal{S}'}_1^\perp$ and $\mathcal{T}'_1 = \mathcal{S}'_1 \cap \mathcal{S}_1^\perp$. Since $\dim \mathcal{S}_1 > \dim \mathcal{S}'_1$ and $\mathcal{S}'_1 \not\subset \mathcal{S}_1^\perp$, we conclude that $\mathcal{T}_1$ is a proper subspace of $\mathcal{S}_1$.

Because $\mathcal{S}_1$ and $\mathcal{S}'_1$ are IrIS's of ϕ, by part (b) of Theorem 3, ϕ fixes the projectors $P_{\mathcal{S}_1}$, $P_{\mathcal{S}'_1}$ and hence also the positive operator $\sigma = P_{\mathcal{S}_1} + 0.5 P_{\mathcal{S}'_1} \in \mathcal{B}(\mathcal{S}_1 + \mathcal{S}'_1)$.

We are going to show that the only eigenvectors of σ with eigenvalue 1 are vectors in the subspace $\mathcal{T}_1$. A vector in $\mathcal{S}_1 + \mathcal{S}'_1$ can be uniquely written as $|\psi\rangle = a|x\rangle + b|x^\perp\rangle$ where $|x\rangle$ and $|x^\perp\rangle$ are normalized vectors in $\mathcal{S}_1$ and $(\mathcal{S}_1 + \mathcal{S}'_1) \cap \mathcal{S}_1^\perp$, respectively. Then $|\psi\rangle$ is an eigenvector of σ with eigenvalue 1 provided that

$$\left(P_{\mathcal{S}_1} + 0.5 P_{\mathcal{S}'_1}\right)\left(a|x\rangle + b|x^\perp\rangle\right) = a|x\rangle + b|x^\perp\rangle. \tag{9}$$

Multiplying $\langle x|$ and $\langle x^\perp|$ to Eq. (9) gives the system of equations

$$\begin{cases} a\langle x|P_{\mathcal{S}'_1}|x\rangle = -b\langle x|P_{\mathcal{S}'_1}|x^\perp\rangle, & \text{(10a)} \\ 0.5a\langle x^\perp|P_{\mathcal{S}'_1}|x\rangle = b\left(1 - 0.5\langle x^\perp|P_{\mathcal{S}'_1}|x^\perp\rangle\right). & \text{(10b)} \end{cases}$$

This system of equations has non-trivial solution if and only if

$$\langle x|P_{\mathcal{S}'_1}|x\rangle\left(1 - 0.5\langle x^\perp|P_{\mathcal{S}'_1}|x^\perp\rangle\right) = -0.5\left|\langle x^\perp|P_{\mathcal{S}'_1}|x\rangle\right|^2. \tag{11}$$

As $P_{\mathcal{S}'_1}$ is a projector, $\langle y|P_{\mathcal{S}'_1}|y\rangle \in [0,1]$ for all normalized vector $|y\rangle$. Therefore, the L.H.S. and R.H.S. of Eq. (11) are non-negative and non-positive, respectively. Consequently, both the R.H.S. and R.H.S. of Eq. (11) equal 0. Thus, $\langle x^\perp|P_{\mathcal{S}'_1}|x\rangle = 0$. Since $1 - 0.5\langle x^\perp|P_{\mathcal{S}'_1}|x^\perp\rangle > 0$, Eq. (10b) implies $b = 0$. So, $|\psi\rangle = a|x\rangle \in \mathcal{T}_1$ is the solution of Eq. (9). In other words, we have succeeded in showing that all eigenvectors of σ with eigenvalue 1 are the vectors in $\mathcal{T}_1$.

Therefore, σ can be rewritten as $P_{\mathcal{T}_1} \oplus \sigma'$ where σ' is a positive operator whose eigenspectrum does not contain the eigenvalue 1 (and hence its support is not in $\mathcal{T}_1$). Using the argument in the proof of part (b) of Theorem 3, we conclude that ϕ fixes $P_{\mathcal{T}_1}$. In other words, $\mathcal{T}_1$ is an proper invariant subspace of $\mathcal{S}_1$. This contradicts the fact that $\mathcal{S}_1$ is irreducible. Therefore, we conclude that $\dim \mathcal{S}_1 = \dim \mathcal{S}'_1$.

To summarize, so far we have deduced that if $\mathcal{S}_i \not\subset {\mathcal{S}'}_j^\perp$ (and hence $\mathcal{S}'_j \not\subset \mathcal{S}_i^\perp$), then $\dim \mathcal{S}_i = \dim \mathcal{S}'_j$. We now construct a finite bipartite graph $\mathfrak{G}$ whose vertices are the IrIS's $\mathcal{S}_i$'s and $\mathcal{S}'_j$'s — each side corresponds to a different IrIS decomposition of $\mathcal{H}$. An edge is drawn between vertices $\mathcal{S}_i$ and $\mathcal{S}'_j$ each picked from one side provided that either (i) $\mathcal{S}_i \not\subset {\mathcal{S}'}_j^\perp$ or (ii) $\mathcal{S}_i = \mathcal{S}'_j$. Our construction of $\mathfrak{G}$ guarantees that:

- Each IrIS must connect to at least one IrIS on the other side of the graph.
- The dimension of each Hilbert space associated with the IrIS's in the same connected component of $\mathfrak{G}$ agrees.
- The direct sum of IrIS's drawn from each of the two sides in a given connect component of $\mathfrak{G}$ must agree.

Since $\mathcal{H}$ is finite-dimensional, we further conclude that in each connected component, the number of IrIS's in the two sides of $\mathfrak{G}$ are the same. Therefore, in each connected component, we can construct a bijection from IrIS's in one side to the IrIS's in the other side of the graph $\mathfrak{G}$. This bijection maps each IrIS in one of the IrIS decomposition to an IrIS of equal dimension in the other decomposition. Hence the theorem is proved. □

Remark 8. *Actually, the construction of the bipartite graph and the determination of the connected components of this graph in the proof of Theorem 4 are quite efficient. To see this, first by Gram-Schmidt orthogonalization procedure, we may represent each subspace* $\mathcal{S}_i$ *of* $\mathcal{H}$ *by its orthogonal basis. Clearly, the computational cost needed to specify all the orthogonal bases of* $\mathcal{S}_i$*'s and* $\mathcal{S}'_j$*'s, measured in terms of the number of real number arithmetical operations, scales like* $O((\dim \mathcal{H})^2)$*. Given a normalized vector* $|v\rangle$ *and a subspace* $\mathcal{S}$ *specified by a set of orthonormal basis* $\{|b_k\rangle\}$*, we may determine if* $|v\rangle$ *is in* $\mathcal{S}$ *or not by checking if* $\sum_i |\langle v|b_i\rangle|^2$ *equal to 1 or not within a certain error tolerant level* ϵ *caused by finite-precision arithmetic. Similarly, we know if* $|v\rangle$ *is in* $\mathcal{S}^\perp$ *or not by checking if* $\sum_i |\langle v|b_i\rangle|^2$ *is equal to 0 or not within a certain error tolerant level* ϵ*. Both procedures require* $O(\dim \mathcal{S}\ \dim \mathcal{H})$ *real number arithmetical operations. Using these procedures as subroutines, we can determine if* $\mathcal{S}_i \not\subset {\mathcal{S}'}_j^\perp$ *or* $\mathcal{S}_i = \mathcal{S}'_j$ *in* $O(\dim \mathcal{S}_i\ \dim \mathcal{S}'_j\ \dim \mathcal{H})$ *time by checking if each basis vector of* $\mathcal{S}$ *is in* ${\mathcal{S}'}_j^\perp$ *or* $\mathcal{S}'_j$*. Hence, the bipartite graph* $\mathfrak{G}$ *described in the proof of Theorem 4 can be constructed in* $\sum_{i,j} O(\dim S_i\ \dim \mathcal{S}'_j\ \dim \mathcal{H}) = O((\dim \mathcal{H})^3)$ *time. Furthermore, connected components of a graph can*

be found by the well-known depth first search algorithm in graph theory, which needs a computational time linear in the number of edges of the graph [18]. So, in our case, connected components of $\mathfrak{G}$ can be determined in at most $O((\dim\mathcal{H})^2)$ time. To summarize, the algorithm concerning the graph $\mathfrak{G}$ in the proof of Theorem 4 takes $O((\dim\mathcal{H})^3)$ time with the graph construction being the most time-consuming step. Thus, the algorithm of identifying isomorphic IrIS decompositions reported in the proof of Theorem 4 is quite efficient and can be used in actual situations especially when $\dim\mathcal{H}$ *is large.*

III. SIMPLE APPLICATIONS OF THE STRUCTURAL THEOREM IN QUANTUM INFORMATION PROCESSING

We report three simple applications of Theorem 3 that are of quantum information science interest. The first one concerns a simplified proof and an extension of the result by Størmer in Ref. [11] on the channel capacity of a unital channel acting on finite-dimensional quantum states. The second one concerns the type of quantum states that are invariant after passing through a unital quantum channel. The third one concerns the preservation of POVM measurement statistics under a unital quantum channel. Our work here strengthens the findings of Arias *et al.* in Ref. [2].

In this Section, ϕ always denotes a unital quantum operation on $\mathcal{B}(\mathcal{H})$ with Kraus operators A_i's and $\dim\mathcal{H} < \infty$.

Theorem 5. *Let $\mathcal{H} = \bigoplus_j \mathcal{S}_j$ be a direct sum decomposition of the Hilbert space $\mathcal{H}$ into IrIS's induced by ϕ. Then*

- *the minimal output α-Renyi entropy ($\alpha \geq 1$) is given by*

$$S_{\min,\alpha}(\phi) = \min_j \left[S_{\min,\alpha}\left(\phi|_{\mathcal{B}(\mathcal{S}_j)}\right)\right], \tag{12a}$$

- *the coherent information is given by*

$$J(\phi) = \max_j \left[J\left(\phi|_{\mathcal{B}(\mathcal{S}_j)}\right)\right], \tag{12b}$$

- *the entanglement-assisted classical capacity is given by*

$$C_e(\phi) = \log \sum_j 2^{C_e(\phi|_{\mathcal{B}(\mathcal{S}_j)})}, \tag{12c}$$

- *the (unassisted) classical capacity is given by*

$$C_{1,\infty}(\phi) = \log \sum_j 2^{C_{1,\infty}(\phi|_{\mathcal{B}(\mathcal{S}_j)})}. \tag{12d}$$

Proof. By Theorem 3, we know that the ϕ can be expressed as a direct sum of finite-dimensional quantum operations. Then, all the above formulae concerning the reduction of various information-theoretic quantities of the quantum operation ϕ follow from Proposition 1 in Ref. [19] by Fukuda and Wolf, which used basic properties such as von Neumann entropy and mutual information are concave functions to show that each of the above capacities can be achieved by a density matrix respecting the direct sum structure of the quantum operation ϕ. □

Remark 9. *Eq.* (12d) *was first proven by Størmer in Theorem 3 of Ref. [11]. The rather complicated conditions in that Theorem is nothing but the structural decomposition of a unital ϕ according to our Theorem 3(b).*

Corollary 3. *The set of all quantum states that are fixed by ϕ are the classical mixtures of the completely mixed states $(\dim\mathcal{S}_j)^{-1} P_{\mathcal{S}_j}$ where each $\mathcal{S}_j$ is an IrIS of ϕ.*

Outline proof. We can always write a density matrix $\rho \in \mathcal{B}(\mathcal{H})$ in the form $\sum_{j=1}^{\dim\mathcal{H}} b_j |y_j\rangle\langle y_j|$ for some orthonormal basis vectors $|y_i\rangle$'s of $\mathcal{H}$ with $b_1 \leq b_j \leq 0$ for all j. Suppose $\phi(\rho) = \rho$. Following the same argument used in the proof of part (b) of Theorem 3, we know that $\rho - b_1 P_{\mathcal{H}}$ is a positive operator fixed by ϕ. Besides, $\mathcal{T} = \operatorname{span}\{|y_j\rangle : b_j = b_1\}$ and $\mathcal{T}' = \operatorname{span}\{|y_j\rangle : b_j \neq b_1\}$ are two mutually orthogonal invariant subspaces of ϕ. As $\mathcal{H}$ is finite-dimensional, by recursively applying this argument to $\rho - b_1 P_{\mathcal{H}}$ and $\phi|_{\mathcal{T}'}$ a finite number of times until $\rho - b_1 P_{\mathcal{H}} = 0$, we conclude that ρ is a finite sum in the form $\sum_j c_j P_{\mathcal{T}_j}$ where $c_j \geq 0$ and $\mathcal{T}_j$'s are mutually orthogonal invariant subspaces of $\mathcal{H}$. Since each $P_{\mathcal{T}_j}$ is (possibly) a classical mixture of completely mixed states in the form $(\dim\mathcal{S}_k)^{-1} P_{\mathcal{S}_k}$'s, this corollary is proved. □

The above corollary means that completely mixed states of IrIS's are the basic building blocks of quantum states fixed by ϕ. In this sense, the problem of finding and characterizing invariant subspaces of ϕ we are studying here is more than a variation of the fixed state problem of ϕ. It is, in fact, a generalization of the fixed state problem.

Remark 10. *Actually, the self-adjointness of ρ is essential in the proof of Corollary 3 while the positivity of ρ is not. So, the Corollary can be slightly extended by saying that all self-adjoint operators that are fixed by ϕ must be in the form $\sum_i a_i P_{\mathcal{S}_i}$ with $a_i \in \mathbb{R}$. Nevertheless, we stress that Corollary 3 does not cover the case of fixing a non-self-adjoint operator — a situation of no physical meaning.*

Remark 11. *Using Theorem 3, Corollary 3 and the fact that a matrix admits two non-orthogonal eigenvectors if and only if it has a degenerate eigenspace, it is easy to see that the following statements are equivalent:*

- *ϕ fixes two non-orthogonal pure states $|x_1\rangle, |x_2\rangle$.*

- *ϕ admits two distinct IrIS decompositions such that the first decomposition contains the IrIS generated by $|x_1\rangle$ and the second decomposition contains the IrIS generated by $|x_2\rangle$.*
- *$|x_1\rangle, |x_2\rangle$ are degenerate eigenvectors of each of the Kraus operators A_i's of ϕ and that $A_i P_{\mathcal{S}} = P_{\mathcal{S}} A_i$ for all i where $P_{\mathcal{S}}$ denotes the projector onto the space spanned by $|x_1\rangle$ and $|x_2\rangle$.*
- *ϕ fixes all pure states in the span of $|x_1\rangle, |x_2\rangle$.*

To address the question of preservation of measurement statistics, we begin with the following lemma.

Lemma 1. *Let Π be a projector on the Hilbert space $\mathcal{H}$. Then*

$$\Pi\, \phi(\rho)\, \Pi^\dagger = \phi\left(\Pi \rho \Pi^\dagger\right) \tag{13}$$

for all $\rho \in \mathcal{B}(\mathcal{H})$ if and only if the image of $\mathcal{H}$ under Π, that is, $\Pi[\mathcal{H}]$, is an invariant subspace of ϕ.

Proof. If $\mathcal{S} \equiv \Pi[\mathcal{H}]$ is an invariant subspace of ϕ, then part (a) of Theorem 3 implies that each Kraus operator of ϕ can be written as $A_i = A_i^{\mathcal{S}} \oplus A_i^{\mathcal{S}^\perp}$ using the notation of that Theorem. Regarding Π and A_i's as block matrices in a basis compatible with the $\mathcal{H} = \mathcal{S} \oplus \mathcal{S}^\perp$ direct sum structure,

$$\begin{aligned}
&\Pi\, \phi(\rho)\, \Pi^\dagger \\
=&\sum_i \begin{bmatrix} I_{\mathcal{S}} & \\ & 0_{\mathcal{S}^\perp} \end{bmatrix} \begin{bmatrix} A_i^{\mathcal{S}} & \\ & A_i^{\mathcal{S}^\perp} \end{bmatrix} \rho \begin{bmatrix} A_i^{\mathcal{S}} & \\ & A_i^{\mathcal{S}^\perp} \end{bmatrix}^\dagger \begin{bmatrix} I_{\mathcal{S}} & \\ & 0_{\mathcal{S}^\perp} \end{bmatrix}^\dagger \\
=&\sum_i \begin{bmatrix} A_i^{\mathcal{S}} & \\ & 0_{\mathcal{S}^\perp} \end{bmatrix} \rho \begin{bmatrix} A_i^{\mathcal{S}\dagger} & \\ & 0_{\mathcal{S}^\perp} \end{bmatrix} \\
=&\sum_i \begin{bmatrix} A_i^{\mathcal{S}} \Pi \rho \Pi^\dagger A_i^{\mathcal{S}\dagger} & \\ & 0_{\mathcal{S}^\perp} \end{bmatrix} \\
=&\sum_i \begin{bmatrix} A_i^{\mathcal{S}} & \\ & A_i^{\mathcal{S}^\perp} \end{bmatrix} \begin{bmatrix} \Pi \rho \Pi^\dagger & \\ & 0_{\mathcal{S}^\perp} \end{bmatrix} \begin{bmatrix} A_i^{\mathcal{S}} & \\ & A_i^{\mathcal{S}^\perp} \end{bmatrix}^\dagger \\
=&\phi\left(\Pi \rho \Pi^\dagger\right)
\end{aligned} \tag{14}$$

for all $\rho \in \mathcal{B}(\mathcal{H})$.

To prove the converse, we observe that $\mathcal{S} = \Pi[\mathcal{H}]$ is a Hilbert subspace of $\mathcal{H}$. For any density matrix $\rho \in \mathcal{B}(\mathcal{S})$, Eq. (13) becomes $\Pi\, \phi(\rho)\, \Pi^\dagger = \phi(\rho)$. Therefore, the density matrix $\phi(\rho) \in \mathcal{B}(\mathcal{S})$. So $\mathcal{S}$ is an invariant subspace of ϕ by definition. □

Theorem 6. *(a) Let $\varphi\colon \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ be the quantum operation $\rho \mapsto \sum_k \Pi_k \rho \Pi_k^\dagger$ where Π_k's are projectors obeying $\sum_k \Pi_k = I_{\mathcal{H}}$ and $\Pi_k \Pi_{k'} = 0$ whenever $k \neq k'$. Then*

$$\varphi \circ \phi(\rho) = \phi \circ \varphi(\rho) \tag{15}$$

for all $\rho \in \mathcal{B}(\mathcal{H})$ if and only if every $\Pi_k[\mathcal{H}]$ is an invariant subspace of ϕ. More importantly,

$$\mathrm{Tr}\left(\Pi_k \rho\right) = \mathrm{Tr}\left[\Pi_k \phi(\rho)\right] \tag{16}$$

for all density matrices ρ in $\mathcal{B}(\mathcal{H})$ and for all k if and only if $\Pi_k[\mathcal{H}]$ is an invariant subspace of ϕ.
(b) More generally, consider a POVM measurement on a quantum state in the Hilbert space $\mathcal{H}$ with POVM elements $\{E_k\}$. (Note that the number of POVM elements need not be finite here.) Then

$$\mathrm{Tr}\left(E_k \rho\right) = \mathrm{Tr}\left[E_k \phi(\rho)\right] \tag{17}$$

for all density matrices ρ in $\mathcal{B}(\mathcal{H})$ if and only if $E_k = \sum_j a_j^{(k)} P_{\mathcal{S}_j}$ with $a_j^{(k)} \geq 0$ where $P_{\mathcal{S}_j}$ is the projector on an IrIS $\mathcal{S}_j$ of ϕ.

Proof. To prove part (a), note that Eq. (15) is a direct consequence of Lemma 1 and linearity of ϕ.

Suppose $\Pi_k[\mathcal{H}]$ is an invariant subspace of ϕ. By taking trace in both sides of Eq. (13) and by using the fact that ϕ is trace-preserving, we have $\mathrm{Tr}\left[\Pi_k \phi(\rho)\right] = \mathrm{Tr}\left[\phi\left(\Pi_k \rho \Pi_k^\dagger\right)\right] = \mathrm{Tr}\left(\Pi_k \rho \Pi_k^\dagger\right) = \mathrm{Tr}\left(\Pi_k \rho\right)$.

To prove the converse in part (a), suppose Eq. (16) holds. We set ρ to an arbitrary but fixed density matrix in $\mathcal{B}(\Pi_k[\mathcal{H}])$. Then, $1 = \mathrm{Tr}\left(\Pi_k \rho\right) = \mathrm{Tr}\left[\Pi_k \phi(\rho) \Pi_k^\dagger\right]$. Since ϕ is trace-preserving and positive, Π_k is a projector and $\dim \mathcal{H}$ is finite, we conclude that $\phi(\rho) \in \mathcal{B}(\Pi_k[\mathcal{H}])$. Hence, $\Pi_k[\mathcal{H}]$ is an invariant subspace of ϕ.

We now move on to prove part (b). The sufficiency condition in part (b) is a direct consequence of part (a) which says that $\mathrm{Tr}\left(P_{\mathcal{S}_j} \rho\right) = \mathrm{Tr}\left[P_{\mathcal{S}_j} \phi(\rho)\right]$ for all IrIS $\mathcal{S}_j$.

To prove the condition is necessary in part (b), we use the fact that each E_k is a positive operator in $\mathcal{B}(\mathcal{H})$ and hence self-adjoint. As $\mathcal{H}$ is finite-dimensional, E_k can be written as the finite sum $\sum_\ell b_\ell P_{\mathcal{T}_\ell}$ where $\mathcal{T}_\ell$'s are mutually orthogonal subspaces of $\mathcal{H}$, $b_\ell > 0$ and $b_\ell < b_{\ell'}$ whenever $\ell > \ell'$. (Surely, b_ℓ's and T_ℓ's depend on k. But we do not explicitly emphasize this dependence to avoid clumsy notations.) Consequently, $\mathrm{Tr}\left(E_k \rho\right) \leq b_1$ for all density matrices $\rho \in \mathcal{B}(\mathcal{H})$ with equality holds if and only if $\rho \in \mathcal{B}(\mathcal{T}_1)$. Let $\rho_1 \in \mathcal{B}(\mathcal{T}_1)$. Eq. (17) implies $\mathrm{Tr}\left[E_k \phi(\rho_1)\right] = b_1$. Hence, $\phi(\rho_1) \in \mathcal{B}(\mathcal{T}_1)$ and $\mathcal{T}_1$ is an invariant subspace of ϕ. By Theorem 3, $\phi\left[\mathcal{B}(\mathcal{T}_1^\perp)\right] \subset \mathcal{B}(\mathcal{T}_1^\perp)$. More importantly, $\mathrm{Tr}\left[E_k \rho'\right] \leq b_2$ for all density matrices $\rho' \in \mathcal{B}(\mathcal{T}_1^\perp)$ with equality holds if and only if $\rho' \in \mathcal{B}(\mathcal{T}_2)$. So, by inductively applying the previous argument, we conclude that all $\mathcal{T}_\ell$'s are invariant subspaces of ϕ. This proves the converse in part (b). □

Remark 12. *The above Theorem says that the order of passing a quantum state through the unital channel ϕ and performing a projective measurement φ on the state is not important provided that $\dim \mathcal{H} < \infty$. Moreover, let us consider the following two machines — the first one performs a POVM measurement on an input quantum state and the second one performs the same POVM measurement after passing the input quantum state through a unital quantum channel. The above Theorem completely characterizes the kind of POVM measurements in the above two machines so that they have the same measurement statistics given any input quantum state. One implication of our findings is that if we do not have control*

on the kind of input quantum states, then measurement statistics may be changed by a unital quantum channel ϕ if the measurement is finer than the direct sum decomposition of the underlying Hilbert space $\mathcal{H}$ into IrIS's of ϕ. This implication echoes with the findings by Blume-Kohout et al.*[12] that the essential geometric structure underlying all noiseless subsystems, decoherence-free subspaces, pointer bases and quantum error-correcting codes on finite-dimensional quantum systems is an isometry to fixed points of certain unital quantum operations.*

IV. DISCUSSIONS

In summary, using elementary analysis and graph theoretic methods, we completely characterize the structure of a unital quantum operation ϕ on $\mathcal{B}(\mathcal{H})$ provided that the Hilbert space $\mathcal{H}$ is finite-dimensional. In particular, the basic building blocks for this kind of unital quantum operations are those without proper IrIS induced by ϕ in the sense that no convex cone formed by the set of all positive semidefinite operators acting on a proper subspace of $\mathcal{H}$ is fixed by ϕ. We further show that although the direct sum decomposition of $\mathcal{H}$ into IrIS's of ϕ need not be unique, the number of IrIS's and the dimension of each IrIS's are unique up to permutation of these IrIS's. Using this structural characterization, we solve three interesting quantum information processing problems, namely, to show a reduction theorem for various information-theoretic capacities of a finite-dimensional unital quantum channel, to find all the fixed states of ϕ, and to give a necessary and sufficient condition for the preservation of measurement statistics of a POVM measurement by ϕ.

Interestingly, we find that the problem of completely characterizing ϕ is reduced to the simultaneous block diagonalization by unitary conjugation of its Kraus operators. Note that in actual practice, this simultaneous block diagonalization can be done relatively painlessly. One possibility is to use a recent computationally stable algorithm reported by Maehara and Murota in Ref. [20], which builds on their earlier works on finding simultaneous invariant subspaces in Refs. [21, 22]. Another possibility is to adapt the algorithm of Blume-Kohout *et al.* in Refs. [12, 13] on finding the so-called information-preserving structures of a quantum channel. Thinking along this direction, the following result of Mendl and Wolf [15] may be of interest. They showed that a unital quantum operation can always be expressed as the sum $\sum_i a_i U_i \cdot U_i^\dagger$ where $a_i \in \mathbb{R}$ obeying $\sum_i a_i = 1$. [15] Note that this is not an operator-sum representation for a_i can be negative. It is instructive to see how to efficiently convert an operation-sum representation of a unital quantum operation ϕ to the above affine sum of unitary conjugations in a computationally stable manner. It is also instructive to see if Kribs' [1] and Arias *et al.*'s [2] necessary and sufficient condition on fixed points of a unital quantum operation restated as Theorem 1 here can be modified to cover the case of the affine sum representation of Mendl and Wolf. Since finding simultaneous diagonal blocks of a set of unitary matrices is much simpler problem, solving the above two problems may improve our computational efficiency and accuracy in finding IrIS's of ϕ.

ACKNOWLEDGMENTS

We would like to thank Debbie W. C. Leung for her valuable discussions. This work is supported under the RGC grant HKU 700709P of the HKSAR Government.

[1] D. W. Kribs, "Quantum channels, wavelets, dilations and representations of $\mathcal{O}_n$," Proc. Edin. Math. Soc. **46**, 421–433 (2003).

[2] A. Arias, A. Gheondea, and S. Gudder, "Fixed points of quantum operations," J. Math. Phys. **43**, 5872 – 5881 (2002).

[3] Hong-Ke Du, Yue-Qing Wang, and Jun-Lian Xu, "Applications of the generalized Lüders theorem," J. Math. Phys. **49**, 013507:1–6 (2008).

[4] Weihua Liu and Junde Wu, "On fixed points of Lüders operation," J. Math. Phys. **50**, 103531:1–2 (2009).

[5] Weihua Liu and Junde Wu, "Fixed points of commutative Lüders operations," J. Phys. A: Math. Theor. **43**, 395206:1–9 (2010).

[6] Yuan Li, "Fixed points of dual quantum operations," J. Math. Anal. and Appl. **382**, 172 – 179 (2011).

[7] Long Long and Shifang Zhang, "Fixed points of commutative super-operators," J. Phys. A: Math. Theor. **44**, 095201:1–10 (2011).

[8] Yuan Li, "Characterizations of fixed points of quantum operations," J. Math. Phys. **52**, 052103:1–9 (2011).

[9] Bebe Prunaru, "Fixed points for Lüders operations and commutators," J. Phys. A: Math. Theor. **44**, 185203:1–2 (2011).

[10] Long Long, "A class of general quantum operations," Int. J. Theor. Phys. **50**, 1319 – 1324 (2011).

[11] E. Størmer, "A reduction theorem for capacity of positive maps," Positivity **11**, 69–75 (2007).

[12] R. Blume-Kohout, H. K. Ng, D. Poulin, and L. Viola, "Characterizing the structure of preserved information in quantum processes," Phys. Rev. Lett **100**, 030501:1–4 (2008).

[13] R. Blume-Kohout, H. K. Ng, D. Poulin, and L. Viola, "Information-preserving structures: A general framework for quantum zero-error information," Phys. Rev. A **82**, 062306:1–25 (2010).

[14] A. Rosmanis, "Fixed space of positive trace-preserving super-operators," (2011), arXiv:1106.3380v2.

[15] C. B. Mendl and M. M. Wolf, "Unital quantum channels — convex structure and revivals of Birkhoff's theorem,"

Comm. Math. Phys. **289**, 1057–1086 (2009).

[16] L. Zhang and J. Wu, "von Neumann entropy-preserving quantum operations," Phys. Lett. A **375**, 4163 – 4165 (2011).

[17] M. A. Nielsen and I. L. Chuang, "Quantum Computation And Quantum Information," (C.U.P., Cambridge, U.K., 2000) pp. 372 – 373, 1st ed., Theorem 8.2.

[18] See, for example, D. Jungnickel, "Graphs, Networks and Algorithms," (Springer, Berlin, 2005) 2nd ed., Chap. 8.2, in particular, Algorithm 8.2.1 and Theorem 8.2.2.

[19] M. Fukuda and M. M. Wolf, "Simplifying additivity problems using direct sum constructions," J. Math. Phys. **48**, 072101:1–7 (2007).

[20] T. Maehara and K. Murota, "Algorithm for error-controlled simultaneous block-diagonalization of matrices," SIAM J. Matrix Anal. Appl. **32**, 605 – 620 (2011).

[21] K. Murota, Y. Kanno, M. Kojima, and S. Kojima, "A numerical algorithm for block-diagonal decomposition of matrix $\star$-algebras with application to semidefinite programming," Japan J. Indust. Appl. Math. **27**, 125–160 (2010).

[22] T. Maehara and K. Murota, "A numerical algorithm for block-diagonal decomposition of matrix $\star$-algebras with general irreducible components," Japan J. Indust. Appl. Math. **27**, 263–293 (2010).